UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,310	06/26/2001	Zheng Qi	2875.0450001	2328

26111 7590 04/20/2007
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/892,310	QI ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-8,11-14,16-21,48-54 and 68-79* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-8,11-14,16-21,48-54 and 68-79* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The indicated allowability of claims 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 are withdrawn in view of the newly discovered reference(s) under 37 CFR 1.97(c) to Kawamura et al. USPN 6,940,975 B1, submitted in the Information Disclosure Statement (IDS) on March 6, 2007. Rejections based on the newly cited reference(s) follow:

Claims Status

2. Claims 1-2, 4, 9-10, 15, 22-45, 47, and 55-67 are previously canceled by the applicant.

3. Claims 3 and 46 are currently cancelled.

4. The applicant currently withdraws claim 80.

5. Claims 5-8, 11-14, 16-21, 48-54, and 68-79 are currently pending.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 5-8, 11-12, 17-21, 48-49, 51-52 and 68-79 are rejected under 35 U.S.C. 102(e) as being anticipated by Kawamura et al. USPN 6,940,975 B1.

Regarding claim 68, Kawamura et al. discloses a cryptography engine (Fig. 13; *DES engine*) for performing cryptographic operations on a data block having a first portion and a second portion (*left, and right 32-bit data blocks*), the cryptography engine comprising:

a key scheduler (fig. 16-18; *key schedulers*) configured to provide a plurality of keys for cryptographic operations (fig. 13; *k1, k2, k3...k16*);

means for combining (fig. 13 *element 85*) via a first logical operation one of the plurality of keys (*k1*) provided by the key scheduler with a first bit sequence (*right 32-bit input data*) to generate a second bit sequence (col. 11 lines 50-55), wherein the first bit sequence is an expansion of the first portion of the data block (col. 11 lines 43-53);

substitution logic (fig. 13 element 84) for receiving the second bit sequence (*combined key and data XOR output*) and for generating a third bit sequence (col. 11 lines 53-55; *substitution output*);

a first inverse permutation logic (fig. 13 element 81b) for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block (*left 32-bits data*) and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round (col. 11 lines 46-49);

a second inverse permutation logic (fig. 13 element 81a) for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block (*right 32-bits data*) and for generating a second inverse permuted bit sequence (col. 11 lines 45-46);

means for combining (fig. 13 element 86) via a second logic operation the third bit sequence (col. 11 lines 55-57; *S-box output*) with the second inverse permuted bit sequence (col.

11 lines 57-59; *left 32-bits output of 81b*) to generate a fourth bit sequence (col. 11 lines 58-60; *right 32-bits on an input to the next round*); and

a permutation logic (fig. 13; *element 83 of the second round*) for permuting the fourth bit sequence (*right 32-bits on an input to the next round*) and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round (col. 11 lines 57-64).

Regarding claim 73, Kawamura et al. discloses an integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block (Fig. 13; *DES engine*) having a first portion and a second portion (*left and right 32-bits data*), the integrated circuit layout comprising:

a key scheduler (fig. 16-18; *key schedulers*) configured to provide a plurality of keys for cryptographic operations (fig. 13; *k1, k2, k3...k16*);

means for combining (fig. 13 *element 85*) via a first logical operation one of the plurality of keys (*k1*) provided by the key scheduler with a first bit sequence (*right 32-bit input data*) to generate a second bit sequence (col. 11 lines 50-55), wherein the first bit sequence is an expansion of the first portion of the data block (col. 11 lines 43-53);

substitution logic (fig. 13 element 84) for receiving the second bit sequence (*combined key and data XOR output*) and for generating a third bit sequence (col. 11 lines 53-55; *substitution output*);

a first inverse permutation logic (fig. 13 element 81b) for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block (*left 32-bits*

data) and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round (col. 11 lines 46-49);

a second inverse permutation logic (fig. 13 element 81a) for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block (*right 32-bits data*) and for generating a second inverse permuted bit sequence (col. 11 lines 45-46);

means for combining (fig. 13 element 86) via a second logic operation the third bit sequence (col. 11 lines 55-57; *S-box output*) with the second inverse permuted bit sequence (col. 11 lines 57-59; *left 32-bits output of 81b*) to generate a fourth bit sequence (col. 11 lines 58-60; *right 32-bits on an input to the next round*); and

a permutation logic (fig. 13; *element 83 of the second round*) for permuting the fourth bit sequence (*right 32-bits on an input to the next round*) and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round (col. 11 lines 57-64).

Regarding claim 78, Kawamura et al. discloses a cryptography engine (Fig. 13; *DES engine*) for performing cryptographic operations on a data block having a first portion and a second portion (*left and right 32-bits data*), the cryptography engine comprising:

a key scheduler (fig. 16-18; *key schedulers*) configured to provide a plurality of keys for cryptographic operations (fig. 13; *k1, k2, k3...k16*);

an expansion logic for expanding the first portion of the data block and for generating a first bit sequence having a first bit size (col. 11 lines 43-53);

a first XOR logic (fig. 13 *element 85*) for performing a first XOR operation of a first key (*k1*) provided by the key scheduler and the first bit sequence (*right 32-bit input data*) and for generating a second bit sequence (col. 11 lines 50-55);

an Sbox logic (fig. 13 element 84) for taking the second bit sequence (*combined key and data XOR output*) and for generating a third bit sequence (col. 11 lines 53-55; *substitution output*) having a second bit size smaller than the first bit size (col. 4 lines 52-65);

a first inverse permutation logic (fig. 13 element 81b) for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block (*left 32-bits data*) and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round (col. 11 lines 46-49);

a second inverse permutation logic (fig. 13 element 81a) for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block (*right 32-bits data*) and for generating a second inverse permuted bit sequence (col. 11 lines 45-46);

a second XOR logic (fig. 13 element 86) performing a second XOR operation of the third bit sequence (col. 11 lines 55-57; *S-box output*) and the second inverse permuted bit sequence (col. 11 lines 57-59; *left 32-bits output of 81b*) to generate a fourth bit sequence (col. 11 lines 58-60; *right 32-bits on an input to the next round*); and

a permutation logic (fig. 13; *element 83 of the second round*) for permuting the fourth bit sequence and generating a permutated bit sequence (*right 32-bits on an input to the next round*), wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round (col. 11 lines 57-64).

Regarding claim 5, Kawamura et al. discloses the cryptography engine wherein the third bit sequence is less than 32 bits (col. 4 lines 53-65).

Regarding claim 6, Kawamura et al. discloses the cryptography engine wherein third bit sequence is four bits (col. 4 lines 60).

Regarding claim 7 Kawamura et al. discloses the cryptography engine wherein the first bit sequence is less than 48 bits (col. 11 lines 45).

Regarding claim 8, Kawamura et al. discloses the cryptography engine wherein the first bit sequence is less than six bits (col. 4 lines 60).

Regarding claim 11, Kawamura et al. discloses the cryptography engine wherein the fourth bit sequence is less than 32 bits (col. 4 lines 53-65).

Regarding claim 12, Kawamura et al. discloses the cryptography engine wherein the fourth bit sequence is four bits (col. 4 lines 60).

Regarding claims 51, and 17-20, Kawamura et al. discloses the integrated circuit layout/ cryptography engine wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage and a consumption stage (fig. 16-18).

Regarding claims 21 and 52 Kawamura et al. discloses the cryptography engine wherein a first shift amount for a first key is identified in the determination stage using a first round counter value (col. 13 lines 10-col. 14 lines 60).

Regarding claim 48, Kawamura et al. discloses the integrated circuit wherein the first bit sequence is four bits (col. 9 lines 36-41).

Regarding claim 49 Kawamura et al. discloses the integrated circuit wherein the expanded first bit sequence is less than six bits (col. 4 lines 53-65).

Regarding claims 69 and 74 Kawamura et al. discloses the cryptography engine/integrated circuit layout wherein the first and second logical operations are binary XOR operation (fig. 13 elements 85, 86).

Regarding claims 70 and 75 Kawamura et al. discloses the cryptography engine/integrated circuit layout wherein the first bit sequence is a bit sequence expanded by an expansion logic (col. 11 lines 43-58).

Regarding claim 71 Kawamura et al. discloses the cryptography engine wherein the third bit sequence is less than the first bit sequence (col. 4 lines 52-65).

Regarding claims 72, 77 and 79 Kawamura et al. discloses the cryptography engine/integrated circuit layout wherein the data block contains bits 0-M, first portion contains bits 0-N, and the second portion contains bits N+1 to M (col. 11 liens 40-50).

Regarding claim 76 Kawamura et al. discloses the integrated circuit layout wherein the second bit sequence is less than the first bit sequence (col. 4 lines 52-65).

8. Claims 13-14, and 53-54, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al. in view of Steinman et al. (Steinman, U.S. Patent No. 6,591,349 B1).

Regarding claims 13 and 53, Kawamura discloses all the subject matter as described above. Kawamura fails to disclose two-level multiplexer. However Steinman teaches the cryptography

engine/integrated circuit layout, further comprising a multiplexer circuitry including a two-level multiplexer (Steinman Col. 4 lines 1-13).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Steinman with in the system of Kawamura because it would allow to increase the performance of computer memory system by reducing lost clock cycles (Steinman Abstract). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level because it would allow to increase the performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. Speeding up the clock cycle improves the performance of DES.

As per claims 14, and 54, the combination teach the cryptography engine/integrated circuit layout wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer (Steinman Col. 4 lines 1-13). The rational for combining are the same as claim 13 above.

9. Claims 16, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura et al. in view of Steinman et al. (Steinman, U.S. Patent No. 6,591,349 B1) and further in view of Teppler (U.S. Patent No. 6,792,536 B1).

As per claims 16, and 50, the combinations teach all the subject matter as described above.

The combination does not explicitly teach performing pipelined key scheduling logic.

However Teppler teaches DES pipelining (Teppler Col. 7 lines 13-25)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Teppler with in the combination system because it would allow to have not impacted system performance (Teppler Col. 7 lines 13-25).

Conclusion

10. Applicant's submission of an information disclosure statement under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p) on March 6, 2007 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

April 12, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

4/13/07